Technology and the protection of personal information

The protection of personal information is a particularly important compliance issue when using technology. You must therefore take all the necessary precautions to avoid unauthorized access to your clients' data. You're responsible for carrying out some of these precautions, while your office manager, broker or IT manager are responsible for others, where applicable, and should be referred to as needed.

Precautions

Physical precautions

- Lock the doors of the rooms where computers, digital devices and servers are located. Lock filing cabinets and secure access to all media (CDs, USB sticks, backup tapes, etc.).

Technology precautions

- Don't open e-mail attachments that look suspicious or where the sender is unknown. Even if your antivirus software is updated, there is always a chance that a new virus is embedded in an attached document. Delete them.
- Switch off workstations or turn on auto sleep.
- Use a password for computers, cellphones, tablets, laptops and USB sticks.
- Set inactive sessions to disconnect.
- Use antivirus software that is regularly updated automatically.
- Use a firewall.
- Schedule automatic software updates to ensure you have the latest versions to benefit from security updates.

In this tool, the masculine gender has been used solely to improve readability.

- Make sure that Bluetooth connections are turned off.
- Avoid sharing (DVDs, CDs, screen, file, printer sharing, remote or management connections online or via Bluetooth). Don't check the "share" box for these services unless specifically required. If so, uncheck the box immediately after sharing. Hackers generally enter systems in this manner.

Encryption

- Encrypt confidential data on computers, laptops and removable media, such as USB sticks. Note that iPhone and iPad data are encrypted, as are newer Android devices. Encryption on older devices must, however, be programmed. Mac computers offer data encryption functions.
- Program your devices to use an SSL connection (a protocol for securing Internet exchanges).
- Program data encryption on your devices before sending.

While away from the office

- Don't discuss a client's case on the telephone in a public place.
- Only lend your computer equipment, used for business purposes, to authorized persons.
- Don't leave your laptop, tablet or cell phone unattended in a car or in a public place.
- Avoid using a public computer or a third-party computer. And if you have to:
  - Use a VPN connection to securely connect to your business computer remotely.
  - Clear your history: downloaded documents (including printed documents, which are downloaded), temporary Internet files, passwords, etc.

Cloud computing

- Try and use cloud services hosted on servers located only on Canadian soil and controlled by Canadian entities. The problem with confidential information hosted on foreign cloud sites is that they are subject to the jurisdiction of the host country rather than to Quebec laws and may thereby be less protected.
- If not dealing with a Canadian entity, encrypt the data at source.
- Perform automatic backups on a regular basis and keep a backup copy of any information hosted on the cloud to ensure it's available in the event of a breakdown or dispute with the cloud service provider.

For information and tips on remote desktop connections and cloud computing, consult the following fact sheets published by the Commission d'accès à l'information du Québec:

- L'infonuagique (ou « Cloud Computing ») [available in French only].
- Guide to the destruction of documents that contain personal information.

Scanning

- Store your clients' scanned information securely.
- Don't share your password with anyone.
- Try and use employees or contractors to scan your client files and have them sign a confidentiality agreement.
- You can also call a firm specializing in document scanning and client management whose servers are ideally located in Quebec.
- For each scanned document, keep some information on paper or in the form of metadata that is added automatically to the file when scanning, if your scanner allows it. This information should be kept throughout the life cycle of the document.
    - The scanner used.
    - The scanning software used.
    - The server where the information is stored.
    - The manufacturer warranties regarding the preservation of data integrity during the transfer between the original document and its digital copy of the scanner.

Agreements with suppliers

- Review carefully any agreement signed with IT service providers (photocopiers, fax machines, data hosting services, Internet access, cloud computing services, etc.), since, as an advisor, you're responsible for the personal information you provide to them.
- Don't allow third parties or service providers to access information from your computer systems without verifying their integrity and without first signing a confidentiality agreement with respect to personal information.
- Consider the possibility of using turnkey solutions that are designed for financial services professionals if you don't know how to implement appropriate protective measures for your client files. You could benefit from economies of scale in this regard.

In case of real risk of harm

If there's a real risk of harm, you should notify the victims, the police, the Commission d'accès à l'information du Québec (Commission) and other parties involved, if necessary. First talk to your firm's or broker's compliance department, where appropriate. They very likely have policies and procedures in place for this purpose. If you don't have access to such a service, you must still take some measures. Don't hesitate to consult the Commission guides and directives:

- To inform the Commission, use the Avis à la Commission d'accès à l'information concernant un incident de confidentialité impliquant des renseignements personnels et qui présente un risque de préjudice sérieux [available in French only].
- You can also consult the Loss or theft of personal information : How shoulf you react? Checklist for citizens and recommend that your clients who are victims of a loss or theft of personal information consult it.

The Commission de l'information Website contains multiple tools related to the protection of personal information such as a Guide d'accompagnement : réaliser une évaluation des facteurs relatifs à la vie privée and an Aide-mémoire sur les nouvelles responsabilités des entreprises, les pistes d'action et les bonnes pratiques (available in French only)

In this tool, the masculine gender has been used solely to improve readability.